A Legal Analysis of S. 968, the PROTECT IP Act

Brian T. Yeh
Legislative Attorney

August 29, 2011

Congressional Research Service
7-5700
www.crs.gov
R41911

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

The global nature of the Internet offers expanded commercial opportunities for intellectual property (IP) rights holders but also increases the potential for copyright and trademark infringement. Piracy of the content created by movie, music, and software companies and counterfeiting of goods such as pharmaceutical drugs and consumer products negatively impacts the American economy and poses risks to the health and safety of U.S. citizens. Although rights holders and law enforcement agencies currently have some legal tools to pursue domestic infringers, they face difficult challenges in enforcing IP laws against actors located abroad. Many websites trafficking in pirated copyrighted content or counterfeit goods are registered and operate in foreign countries. These foreign "rogue sites" sell or distribute subject matter protected by federal IP laws to people located within the United States—without the authorization of the IP rights holders—yet the operators of the sites remain beyond the reach of U.S courts and authorities.

Some believe that legislation is necessary to address this jurisdictional problem. In 2010, the Combating Online Infringement and Counterfeits Act (COICA) was approved by the Senate Judiciary Committee, but the full Senate took no action on the bill before the end of the 111th Congress. On May 12, 2011, Senator Leahy introduced S. 968, the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PROTECT IP Act), which is similar to COICA in several respects. The act would allow the Attorney General to seek an injunction from a federal court against a domain name used by a foreign website that promotes infringement or the sale of counterfeit goods; such court order may then be served on U.S.-based domain name servers, Internet advertisers, search engines, and financial transaction providers, which would be required to take certain appropriate actions such as preventing access to the website or suspending business services to the site. The Senate Judiciary Committee voted to report S. 968 to the full Senate on May 26, 2011.

There has been considerable public debate about the PROTECT IP Act. Critics claim it is an "internet censorship" bill and that it tramples on free speech rights. There are also concerns that focusing on intermediary services, such as non-authoritative domain name servers, will disrupt the technical integrity of the Internet. Opponents of the bill believe that these problems will be exacerbated by the legislation's inclusion of a private cause of action allowing content owners to sue intermediate service providers. Supporters of the legislation, however, argue that in order to reduce digital piracy and online counterfeiting committed by foreign websites, new enforcement mechanisms are vital for U.S. economic growth and needed to protect public health and safety.

Contents

Introduction 1
Legislative History of COICA (111th) and PROTECT IP (112th) 2
Summary of PROTECT IP Provisions 2
Concerns Raised About the PROTECT IP Act 5
Impact on Free Speech 5
Technical Integrity of the Internet 6
Private Cause of Action 7

Contacts

Author Contact Information 8
Acknowledgments 8

Introduction

The Internet has become a central part of the American economy, delivering innovative products while eliminating the need for inefficient middlemen. However, the free flow of information facilitated by the Internet has also created problems with copyright and trademark infringement. The problem is significant; as much as 6% of the U.S. gross national product is generated by industries supported by intellectual property laws.[1] A recent report contends that nearly 24% of all Internet traffic worldwide is infringing.[2] Piracy of the content created by movie, music, and software companies, and counterfeiting of goods such as clothing, pharmaceutical drugs, and consumer electronics, negatively impacts the American economy.[3] Although the Government Accountability Office cautions that it is difficult to precisely quantify the economy-wide impacts of piracy, it is believed to be a serious problem.[4]

To combat problems with online copyright and trademark infringement, U.S. Immigration and Customs Enforcement (ICE) began a new initiative called "Operation In Our Sites." Between June 30, 2010, and February 14, 2011, ICE seized 112 domain names[5] associated with Internet piracy.[6] Domain name seizures are an innovative use of civil forfeiture proceedings authorized under criminal copyright law.[7] Domain name registrars redirected traffic from the seized domains to a government website explaining that the domain name had been seized by ICE pursuant to a warrant issued by a federal court. However, the sites remain online and accessible through their Internet protocol addresses.[8]

---

[1] *Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part II: Hearing Before the Subcomm. on Intellectual Property, Competition and the Internet of H. Comm. on the Judiciary,* 112th Cong. (2011) (written statement of Frederick Huntsberry, Chief Operating Officer Paramount Pictures Corp.).

[2] *See Targeting Websites Dedicated To Stealing American Intellectual Property: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. (2011) (written statement of Sen. Patrick Leahy, Chairman S. Comm. on the Judiciary, *citing* a report commissioned by NBC Universal, available at http://documents.envisional.com/docs/Envisional-Internet_Usage-Jan2011.pdf).

[3] As used in this report, the term "piracy" refers to the unlawful reproduction and distribution of copyrighted content, and "counterfeiting" refers to the manufacture and distribution of products that bear (without authorization) a trademark that is identical to a trademark validly registered for those goods, or that cannot be distinguished in its essential aspects from such a trademark, and that, thereby, infringes the rights of the owner of the trademark in question. These definitions are adapted from those used in the World Trade Organization (WTO)'s Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement), Section 4, Article 51, footnote 14, available at http://www.wto.org/english/tratop_e/trips_e/t_agm4_e.htm#Footnote14.

[4] U.S. Government Accountability Office, *Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods*, 10-423, April 2010, p. 2, available at http://www.gao.gov/new.items/d10423.pdf.

[5] A domain name can be typed into a web browser to access an Internet address; it usually consists of a "top level domain" and a "second level domain"—for example, in the domain name "amazon.com," ".com" is a top level domain, and "amazon" is the second level domain. A domain name registry operates top level domains, and a domain name registrar manages the registration of domain names. See S.Rept. 111-373 at 6 (discussing a predecessor bill).

[6] *Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part II: Hearing Before the Subcomm. on Intellectual Property, Competition and the Internet of H. Comm. on the Judiciary,* 112th Cong. (2011) (written statement of Hon. John Morton, Dir. U.S. Immigration and Customs Enforcement.).

[7] *See* 18 U.S.C. § 2323 (allowing civil forfeiture for "Any property used, or intended to be used, in any manner or part to commit or facilitate the commission of [criminal copyright infringement].").

[8] An Internet protocol address is a series of numbers assigned to a device attached to a network. These numbers are used to indicate where the device is located on the network. For example, when a user visits http://www.google.com the user's computer is communicating with 74.125.93.147, the Internet protocol address of google.com's webserver.

The global nature of the Internet presents problems to the civil forfeiture approach. Only domain names registered within the United States and subject to ICE's jurisdiction may be seized. However, many websites trafficking in copyrighted content or counterfeit goods are registered and operate entirely in foreign countries. These foreign "rogue sites" often provide content protected by U.S. intellectual property law to people located within the United States. S. 968, the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PROTECT IP Act), is a legislative response to this jurisdictional problem. The act restricts access to foreign sites promoting infringement or the sale of counterfeit goods by targeting domain name servers, Internet advertisers, and financial transaction providers located in the United States. There has been considerable public debate about this approach.

Legislative History of COICA (111th) and PROTECT IP (112th)

On September 20, 2010, Senator Leahy with Senator Hatch introduced the Combating Online Infringement and Counterfeits Act (COICA). COICA is a predecessor to the PROTECT IP Act and follows a similar legislative approach, though with some significant differences. The Senate Judiciary Committee voted to report COICA favorably to the Senate, with an amendment in the nature of a substitute. However, no public hearing was held to consider COICA before the end of the 111th Congress, and the full Senate did not act on the legislation before the end of the congressional term.

At the request of Senator Coburn, the Senate Judiciary Committee in the 112th Congress held a hearing February 16, 2011, on the topic of "Targeting Websites Dedicated To Stealing American Intellectual Property." This hearing considered the scope of intellectual property theft over the Internet and the problem of "rogue websites" that exclusively traffic in infringing material, issues that COICA was designed to address.[9]

On May 12, 2011, Senator Leahy introduced the PROTECT IP Act. On May 26, 2011, the Senate Committee on the Judiciary voted to report the legislation to the full Senate, with an amendment in the nature of a substitute and without written report.[10] Senator Wyden then placed a hold on the bill, indicating his intent to object to any unanimous consent request to proceed.[11] The Senate Judiciary Committee held a hearing on June 22, 2011, entitled "Oversight of Intellectual Property Law Enforcement Efforts" that included testimony from ICE and other agencies charged with enforcement of intellectual property laws online.

Summary of PROTECT IP Provisions

The following is a brief summary of the key provisions of S. 968, as reported in the Senate.

[9] Nathan Pollard and Amy E. Bivins, *Leahy Vows to Offer Tough Anti-Piracy Bill; Senator Demands 'Accountability' From ISPs*, 16 Electronic Commerce & Law Report 257 (Feb. 23, 2011).

[10] Sen. Leahy, Report of the Sen. Judiciary Committee, *Congressional Record*, May 26, 2011, p. S3426.

[11] Sen. Wyden, Intent to Object, *Congressional Record*, May 26, 2011, p. S3419.

- The act focuses on Internet sites "dedicated to infringing activities." An "Internet site dedicated to infringing activities," as defined by the bill, is an Internet site that has no significant use other than engaging in, enabling, or facilitating: (1) copyright infringement, (2) circumvention of copyright protection systems, or (3) the sale, distribution, or promotion of goods, services, or materials bearing a counterfeit mark. The term also encompasses websites which facts or circumstances suggest are used primarily as a means for engaging in or enabling those activities.[12] The act also defines "Nondomestic domain name" as a domain name for which the domain name registry is not located in the United States.[13]
- The Attorney General may bring suit against a person who registers or owns a nondomestic domain name used by an Internet site dedicated to infringing activities.[14] This provision is unlikely to be invoked often because registrants of nondomestic domain names are rarely located in the United States and are therefore difficult to prosecute domestically.
- The Attorney General is authorized to initiate civil forfeiture proceedings against a nondomestic domain name used by an Internet site dedicated to infringing activities. In response, a federal court may issue an injunction against the domain name if the domain name is used within the United States and the Internet site harms holders of U.S. intellectual property rights.[15] Should the court grant the injunction, a federal law enforcement officer (with prior court approval) may serve a copy of the court order to the following entities that would be required to take the specified actions:
    - **Operators of non-authoritative domain name servers:** Non-authoritative domain name servers are intermediary servers used to resolve a domain name to its Internet protocol address. They do this by retaining a copy of information stored on an authoritative domain name server. Operators of these servers, generally Internet service providers, are directed to prevent access to seized domain names through the least burdensome technically feasible means.[16]
    - **Financial transaction providers:** Companies that facilitate online transactions, such as credit card companies, are required to prevent their service from completing transactions between customers located within the United States and the Internet site.[17]
    - **Internet advertising services:** Internet advertising services are required to stop selling advertising to and providing advertising for the Internet site.[18]

[12] S. 968 as reported, §2 (7).

[13] S. 968 as reported, §2 (9).

[14] S. 968 as reported, §3 (a) (1).

[15] The injunction proceedings must conform with Rule 65 of the Federal Rules of Civil Procedure. *See* S. 968 as reported, §§ 3 (a) (2) – (b).

[16] S. 968 as reported, §3 (d) (2).

[17] *Id.*

[18] *Id.*

- **Information location tools:** Search engines such as Google and Yahoo must take technically feasible measures to remove or disable access to the Internet site.[19]

- A qualifying plaintiff[20] may bring suit against a person who registered a domain name used by an Internet site dedicated to infringing activities. This provision gives a private right of action to rights holders against registrants of domestic and nondomestic domain names.[21]

- A qualifying plaintiff may also bring suit against a nondomestic domain name used by an Internet site dedicated to infringing activities. In response, a federal court may issue an injunction against the domain name if the domain name is used within the United States to access the Internet site and the site harms holders of U.S. intellectual property rights.[22] Should the court grant the injunction, the qualifying plaintiff (with prior court approval) may serve a copy of the court order to the following entities, which would then be responsible for taking the specified actions:

  - **Financial transaction providers:** Companies that facilitate online transactions, such as credit card companies, are required to prevent their service from completing transactions between customers located within the United States and the Internet site.[23]

  - **Internet advertising services:** Internet advertising services are required to stop selling advertising to and providing advertising for the Internet site.[24]

- Any person bound by a court order (registrant of the domain name, owner/operator of the Internet site, financial transaction provider, Internet advertising service) may file a motion with the court to modify, suspend, or vacate the order; the court may grant such relief if the court finds that either (1) the Internet site associated with the domain name no longer, or never was, dedicated to infringing activities, or (2) the interests of justice require it.[25]

- To encourage financial transaction providers and Internet advertising services to "self-police," the act makes them immune from liability for voluntarily taking action against an Internet site, so long as they act in good faith on credible evidence that the Internet site is dedicated to infringing activities.[26]

- The act provides immunity from liability to more actors when they refuse to provide services to "infringing Internet sites that endanger the public health." An

[19] *Id.*

[20] A qualifying plaintiff is defined by the bill as (1) the U.S. Attorney General or (2) "an owner of an intellectual property right ... harmed by the activities of an Internet site dedicated to infringing activities occurring on that Internet site." *See* S. 968 as reported, §2 (11) (B).

[21] S. 968 as reported, §4 (a).

[22] The injunction proceedings must be in accordance with Rule 65 of the Federal Rules of Civil Procedure. *See* S. 968 as reported, §4 (b) (1).

[23] S. 968 as reported, §4 (d) (2).

[24] *Id.*

[25] S. 968 as reported, §4 (f).

[26] S. 968 as reported, §5 (a).

"infringing Internet site that endangers the public health" is an Internet site that sells, dispenses, or distributes counterfeit prescription medicine. Domain name registries, domain name registrars, financial transaction providers, search engines, and Internet advertising services may refuse to provide services to such Internet sites when they have a good faith belief that the site is infringing.[27]

- Finally, the bill requires reports to Congress regarding the effectiveness of the act and its effect on Internet technologies, from the following government entities: the Attorney General, the Register of Copyrights, the Secretary of Commerce, and the Government Accountability Office.

Concerns Raised About the PROTECT IP Act

Numerous concerns have been raised by consumer groups and privacy advocates about the provisions of the PROTECT IP Act. These concerns, and the responses by the legislation's supporters, can be organized broadly into the following three categories.

Impact on Free Speech

Some commentators are concerned that the broad definition of an Internet site dedicated to infringing activity could encompass speech protected by the First Amendment.[28] A *New York Times* editorial opined that "the broadness of the definition is particularly worrisome."[29] Others claim that it will give owners of copyrighted content "broad censorship powers."[30] These concerns are heightened by fears that the act provides insufficient legal process prior to seizure.

Opponents of the bill argue that repressive foreign regimes could cite U.S. domain name seizures to justify online suppression of speech. Eric Schmidt, executive chairman of Google, compared the domain name seizure approach to China's attempts to stifle free speech. He warned that the act could set a disastrous precedent if done the wrong way.[31] There is concern that backing away from an open and global Internet could set "a precedent for other countries ... to use DNS [domain name system] mechanisms to enforce a range of domestic policies, erecting barriers on the global medium of the Internet. Non-democratic regimes could seize on the precedent to justify measures that would hinder online freedom of expression and association."[32]

Supporters of the bill note that "[a]ll existing copyright protections are applicable to the Internet" and that "injunctions are a longstanding, constitutionally sanctioned way to remedy and prevent

[27] S. 968 as reported, §5 (b).

[28] Letter from Mark Lemley, Professor, Stanford Law School, et al. to Sen. Judiciary Comm. (June 27, 2011) available at http://volokh.com/2011/07/04/and-speaking-of-the-inalienable-right-to-the-pursuit-of-happiness.

[29] Editorial, "Internet Piracy and How to Stop It," *New York Times*, June 9, 2011, p. A26.

[30] Mike Masnick, *Son of COICA*, Techdirt, May 10, 2011, http://www.techdirt.com/articles/20110510/13285714230/.

[31] Nathan Olivarez-Giles, "Google's Eric Schmidt: Blocking File-sharing Sites Would Make U.S., Britain like China," *Los Angeles Times,* May 18, 2011, available at http://latimesblogs.latimes.com/technology/2011/05/google-eric-schmidt-says-blocking-filesharing-sites-would-make-u-s-u-k-ike-china.html.

[32] Letter from Center for Democracy and Technology et al. to Sen. Patrick Leahy, Chairman Sen. Judiciary Comm. (May 25, 2011) available at http://www.cdt.org/files/pdfs/20110525_public_interet_968_ltr.pdf.

copyright violations."[33] The Register of Copyrights does not believe that seizing an infringing domain name would violate the First Amendment or that it constitutes censorship.[34] Supporters also point to Supreme Court precedents in favor of injunctions for copyright infringement, even when the copyrighted material is a matter of public debate.[35] However, it is probable that a narrowly tailored definition of an infringing site is less likely to implicate First Amendment concerns.

Technical Integrity of the Internet

Opponents of the PROTECT IP Act have raised concerns that the bill may affect the integrity of the Internet.[36] "DNS blocking itself could affect the Internet's reliability, security, and performance."[37] Other commentators have called the domain name blocking approach ineffective.[38] They argue that the Internet sites will remain available through their Internet protocol addresses:

> [D]omain name address resolution takes place throughout the Internet, not just by larger ISPs and registries. Indeed, there are as many as a million worldwide domain names "resolvers," and it is unlikely U.S. courts could or would order all of them to comply with a blocking order. But incomplete blocking could seriously undermine the integrity of this key feature of the Web's architecture, incentivizing truly rogue Web site operators to use shadow registration systems or simply forgo domain names and rely solely on IP addresses.[39]

Supporters respond that taking down infringing Internet sites is akin to "whac-a-mole" and that the law must provide sufficient authority to combat this problem.[40] Furthermore, supporters believe the DNS blocking provisions of the bill are key to preventing foreign sites from infringing American intellectual property rights:

---

[33] *Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part II: Hearing Before the Subcomm. on Intellectual Property, Competition and the Internet of H. Comm. on the Judiciary,* 112th Cong. (2011) (written statement of Floyd Abrams, Partner, Cahill Gordon & Reindel LLP).

[34] *Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part I: Hearing Before the Subcomm. on Intellectual Property, Competition and the Internet of H. Comm. on the Judiciary,* 112th Cong. (2011) (written statement of Maria Pallante, Acting Register of Copyrights).

[35] *Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part II: Hearing Before the Subcomm. on Intellectual Property, Competition and the Internet of H. Comm. on the Judiciary,* 112th Cong. (2011) (written statement of Floyd Abrams, Partner, Cahill Gordon & Reindel LLP *citing Harper & Row v. Nation Enters.*, 471 U.S. 539 (1985) (finding an injunction against a magazine's infringing publication of portions of Gerald Ford's memoir valid)).

[36] Letter from Internet Engineers Opposed to COICA, to Sen. Judiciary Comm. (Sept. 28, 2010) available at http://www.publicknowledge.org/files/docs/COICA_internet_engineers_letter.pdf (discussing similar provisions in a preceding bill).

[37] *Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part II: Hearing Before the Subcomm. on Intellectual Property, Competition and the Internet of H. Comm. on the Judiciary,* 112th Cong. (2011) (written statement of Kent Walker, Senior Vice President, Google).

[38] *See e.g.* Editorial, "Internet Piracy and How to Stop It," *New York Times*, June 9, 2011, p. A26; Editorial, "Policing the Internet", *Los Angeles Times,* June 7, 2011, available at http://articles.latimes.com/2011/jun/07/opinion/la-ed-protectip-20110607.

[39] Larry Downes, *Leahy's Protect IP Bill Even Worse than COICA,* CNET News (June 20, 2011 2:46 p.m.), http://news.cnet.com/8301-13578_3-20062419-38.html.

[40] The references to "whac-a-mole" are ubiquitous. *See e.g. Targeting Websites Dedicated To Stealing American Intellectual Property: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. (2011) (written statement of Tom Adams, Chief Executive Officer, Rosetta Stone).

> Reaching sites originating outside the U.S. is critical to fighting a worldwide epidemic that is destroying the ability of the [content owners] to obtain the financing needed to produce future [content]. ... Internet sites that steal and distribute American intellectual property are often foreign-owned and operated, or reside at domain names that are not registered through a U.S.-based registry or registrar, setting them outside the scope of U.S. law enforcement. The Justice Department and rights holders are currently limited in their options for legal recourse, even when the website is directed at American consumers and steals American-owned intellectual property.[41]

Private Cause of Action

There is considerable consternation from opponents of the bill that these problems will be exacerbated by including a private cause of action. They worry that content owners will use the private right of action to stifle Internet innovation and protect outdated business models.[42] "[T]he Internet and digital technologies can be highly disruptive of traditional business models for reasons having nothing to do with infringement."[43] Additionally, technology companies are concerned that they will be unable to cope with thousands of suits from content owners. They argue that these suits will overwhelm their ability to handle requests and ultimately increase costs for consumers.[44] "We believe that the currently proposed private litigation-based process will, however unintentionally, become a one-sided litigation machine with rights owners mass-producing virtually identical cases against foreign domain names for the purpose of obtaining orders to serve on U.S. payment and advertising companies."[45] Instead, some technology companies have proposed a system of legal safe harbors similar to the notice and takedown provisions of the Digital Millennium Copyright Act.[46]

Proponents of the act argue that online infringement is rampant and that law enforcement lacks the resources to deter infringing activities. Additionally, they pointed out that remedies in private actions are limited to payment processors and online advertisers; only the Attorney General can bring suit against domain name servers and search engines. These limitations, they argue, are sufficient to prevent an explosion of litigation.

---

[41] Press Release, The Motion Picture Association of America, Broad Creative Industry Coalition Praises Senate Introduction of Bipartisan Legislation to fight Online Theft (May 12, 2011) available at http://mpaa.org/resources/e62fa607-8234-4120-97f2-aa4082cd691a.pdf.

[42] *See* Abigail Phillips, *The "PROTECT IP" Act: COICA Redux, The* Electronic Frontier Foundation (June 20, 4:31 p.m.), https://www.eff.org/deeplinks/2011/05/protect-ip-act-coica-redux (wondering whether Viacom would have quashed YouTube had the bill been law at the time).

[43] *Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part I: Hearing Before the Subcomm. on Intellectual Property, Competition and the Internet of H. Comm. on the Judiciary,* 112th Cong. (2011) (written statement of David Sohn, Senior Policy Counsel, Center for Democracy and Technology).

[44] See *Targeting Websites Dedicated To Stealing American Intellectual Property: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. (2011) (written statement of Thomas Dailey, General Counsel, Verizon).

[45] Letter from American Express et al. to Sen. Patrick Leahy, Chairman, Sen. Judiciary Comm. (May 25, 2011) available at http://www.publicknowledge.org/letter-opposing-PIPA-privaterightofaction.

[46] See *Targeting Websites Dedicated To Stealing American Intellectual Property: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. (2011) (written statement of Kent Walker, Senior Vice President and General Counsel, Google). For more information regarding this system, *see* CRS Report RL32037, *Safe Harbor for Service Providers Under the Digital Millennium Copyright Act*, by Brian T. Yeh and Robin Jeweler.

Author Contact Information

Brian T. Yeh
Legislative Attorney
byeh@crs.loc.gov, 7-5182

Acknowledgments

Portions of this report were prepared by Jonathan H. Miller, Law Clerk, American Law Division.